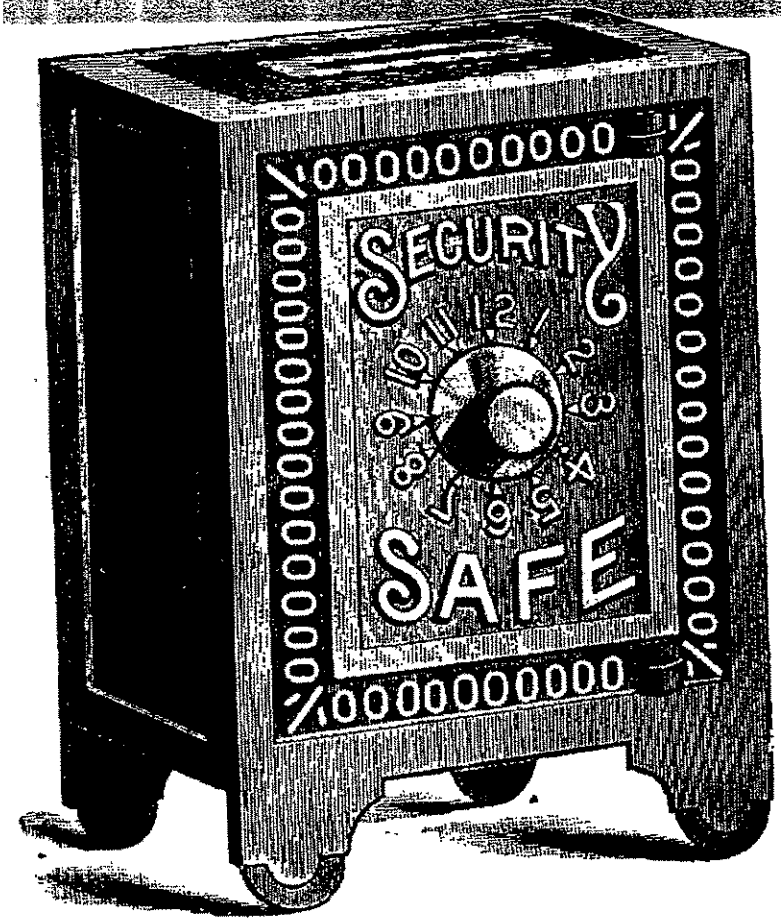
Computer Security

2nd Edition
Expanded & Updated

Practical UNIX & Internet Security



O'REILLY®

Simson Garfinkel and Gene Spafford

Practical UNIX & Internet Security

Garfinkel & Spafford

Anatomy of a Firewall

Fundamentally, all firewalls consist of the following two kinds of components:*

Chokes

Computer or communications devices that restrict the free flow of packets between networks. Chokes are often implemented with routers, but they do not have to be. The use of the word "choke" is taken from the field of electronics: a choke is a device that exhibits great resistance to certain types of signals, but not to others.

Gates

Specially designated programs, devices, or computers within the firewall's perimeter that receive connections from external networks and handle them appropriately. Other texts on firewalls sometimes refer to single machines that handle all gate functions as *bastion hosts*.

Ideally, users should not have accounts on a gate computer. This restriction helps improve the computer's reliability and users' security.

On the gate(s), you may run one or more of the following kinds of programs:

Network client software

Client software includes programs such as *telnet*, *ftp* and *mosaic*. One of the simplest ways to give users limited access to the Internet is to allow them to log onto the gate machine and allow them to run network client software directly. This technique has the disadvantage that you must either create user accounts on the gate computer, or you must have users share a single account.

Proxy server

A proxy is a program that poses as another. In the case of a firewall, a proxy is a program that forwards a request through your firewall, from the internal network to the external one.

Network servers

You can also run network servers on your gate. For example, you might want to run an SMTP server such as *sendmail* or *smap* so that you can receive electronic mail. (If you wish to run an HTTP server to publish information on the World Wide Web, that server should be run on a separate computer, and *not* on your gate.)

Many network servers can also function as proxies. They can do so because they implement simple store-and-forward models, allowing them to forward queries or

* The first edition of this book introduced this terminology as part of one of the first written descriptions of firewalls. Although not everyone in the community has adopted these terms, we believe that they are at least as descriptive as other terms invented since.